REMARKS

Claims 1-8 are pending in the above-identified patent application. Claims 1, 3 and 5 have been amended by way of the present amendment. Reconsideration is respectfully requested.

In the outstanding Office Action, **FIG. 1**, **FIG. 2A** and **FIG. 2B** were indicated as needing to be designated with a legend, such as: "Prior Art"; the specification was indicated as having a typographical error for stating "**FIG. 2**" instead of "**FIG. 2A**"; a more descriptive title was suggested; the Abstract was objected to for referencing numbered elements in the figures; claim 1 was objected to due to informalities; claims 1-2 and 6-8 were rejected under 35 U.S.C. Section 112, 2nd paragraph; claims 1-8 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,016,350 (Funable et al.) in view of U.S. Patent No. 7,076,651 (Droge). Reconsideration is respectfully requested.

Drawing Amendments

In the drawings, **FIG. 1**, **FIG. 2A** and **FIG. 2B** were indicated as needing to be designated with a legend, such as: "Prior Art." The drawings have been amended to include the legend: "Background Art." Replacement sheets for **FIG. 1**, **FIG. 2A** and **FIG. 2B** are attached hereto and filed herewith that include the amendment. It is respectfully submitted that the amendment raises no questions of new matter.

Specification Amendments

The specification was indicated as having a typographical error for stating "**FIG. 2**" instead of "**FIG. 2A**"; a more descriptive title was suggested; and the Abstract was objected to for referencing numbered elements in the figures. Reconsideration is respectfully requested.

The specification has been amended at paragraph **[0026]** to correct the typographical error and now states "**FIG. 2A**" instead of "**FIG. 2**". The title of the application was replaced by the title suggested in the outstanding Office Action. The Abstract was amended to delete the reference numbers of elements in the figures from the text. Thus, it is respectfully submitted that the outstanding items have been addressed and that the specification is now in a proper form.

Claim Objections

Claim 1 was objected to due to informalities. Claim 1 has been amended to clarify the invention in language similar to that suggested in the outstanding Office Action. Thus, it is respectfully submitted that the informalities have been addressed and respectfully requested that the outstanding claim objection be withdrawn.

35 U.S.C. § 112 Claim Rejections

Claims 1-2 and 6-8 were rejected under 35 U.S.C. Section 112, 2nd paragraph. Claim 1 has been amended to provide proper antecedent basis for the term "non-encrypting capability." Thus, it is respectfully submitted that claim 1, and claims dependent thereon are now definite and it is respectfully requested that the outstanding rejections to claim 1 and claims dependent thereon, be withdrawn.

35 U.S.C. § 103 Claim Rejections

Claims 1-8 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Funable et al. in view of Droge. Reconsideration is respectfully requested.

Claims 1, 3 and 5 have been amended to clarify the invention. In particular, claim 1 has been amended to recite:

> bridge means in a data link layer for allowing data, which has been received with one of the plurality of ports and then on which the encrypting or decrypting process has been performed, to be outputted as it is from another port without ~~being performed~~ any routing process at a network layer being performed.

Independent claims 3 and 5 state similar limitations. In addition, new dependent claims 9-11 have been added to further clarify the invention. Support for the amendments and new claims is provided by the original specification and figures. In particular, as shown in **FIG. 7,** the DB

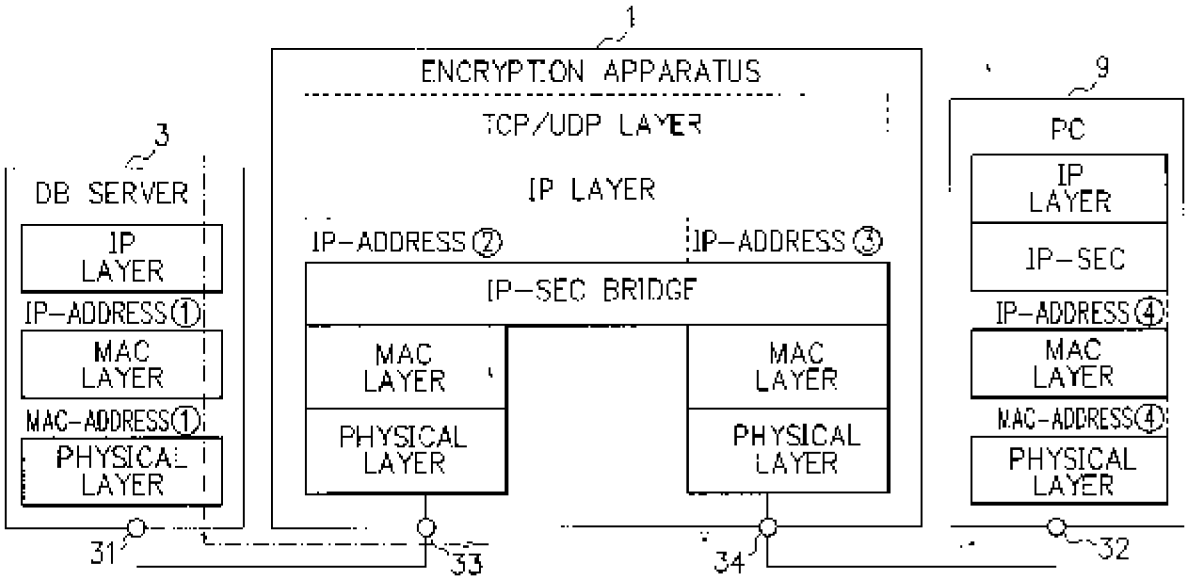
server **3** and the PC **9** have ports **31** and **32**, respectively. Further, the encryption apparatus **1** in **FIG. 7** is designed so as to function as a relay device with two ports **33** and **34**. In the encryption apparatus **1**, the physical layer and the MAC layer (data link layer) are provided for each of the ports **33** and **34**. In addition, in the encryption apparatus **1**, for the ports **33** and **34**, the IP-Sec (encrypting/decrypting capability), the IP layer (network layer) and the TCP/UDP layer (transport layer) are provided. As a result of this arrangement, the encryption apparatus **1** of this embodiment is characterized in that the IP-Sec serves as the recited "bridge means" that links the ports **33** and **34** in the encryption apparatus **1**.

Specifically, the specification discloses the term "bridge" indicates a function of sending data just as it is (which has inputted therein via one of the ports and then on which the encrypting or decrypting process has been performed) to another port without performing any routing process. That is, as shown in **FIG. 7**, data is inputted via the first port **33** in the encryption apparatus **1**, and then the decrypting process is performed on the inputted data at the IP-Sec. Further, the specification discloses:

> *without performing on the encrypted data any routing process at the IP layer*, the encrypted data (just as it is) is sent to and outputted from the second port **34**. (In other words, without passing the encrypted data to the IP layer, the data after the decryption, just as it is, is sent to and outputted from the second port 34.) This manner corresponds to the abovementioned "bridge" process. Namely, in the encryption apparatus 1 according to the present embodiment, the IP layer and the TCP/UDP layer are not used in *the data transmission between the DB server 3 and the PC 9, and the data transmission process is carried out in layers lower than the IP layer* (emphasis added).

Thus, in consideration of the above-discussion, it is respectfully submitted that the amendments and the new claims raise no questions of new matter.

FIG. 7



Funabe et al. discloses an encryption apparatus enables encrypted communications using existing network equipment which does not have an encryption function, such as a server, a client, or a router.[1] However, as indicated at page 5, line 6 of the outstanding Office Action, Funabe et al. nowhere discloses, "bridge means in a data link layer" (i.e., a communication device in the data link layer), but instead discloses a communication device in the upper layers (i.e., in the network layer/transport layer) including IXP, RIP, SAP, etc. While a VPN router (i.e., an encryption communication device in the network layer) is the well-known technology/product in general as the encryption communication device located in the transport layer or network layer, the claimed invention realizes an IPsec=IP network encryption communication (i.e., encryption communication in the network layer) as a bridge means (i.e., communication in the data link layer). Thus, it is respectfully submitted that Funabe et al. does not disclose all of the limitations of claims 1, 3 and 5.

[1] Funabe et al. at ABSTRACT.

As discussed above, the outstanding Office Action acknowledges these deficiencies in Funabe et al. and attempts to overcome these deficiencies by combining Droge with Funabe et al. However, Droge cannot overcome all of the deficiencies of Funabe et al., as discussed below.

Droge discloses a system and method for highly secure data communication that may include encrypting data a first time, packetizing the data, encrypting the data a second time and transmitting the data.[2] Generally, Droge provides an overview of the Open System Interconnect (OSI) reference model that describes how data in one computer or interface device is transferred through a network to another computer. Specifically, the OSI reference model comprises seven layers, each layer specifying a function of the network and comprises an application layer, a presentation layer, a session layer, a transport layer, a network layer, a data link layer, and a physical layer. In addition, Droge discloses data that is transferred from, for example a software application in one computer (i.e., at the application layer) to another computer must pass down through each layer of the OSI reference until the data is transferred to the physical layer. Further, Droge discloses the receiving computer would receive the data at the physical layer and transfer the data up through the OSI reference model layers until the data exists as a document in the word processing application on the receiving computer. In particular, as shown in **FIG. 3** below and as discussed in the specification, Droge discloses data may be encrypted at a data link layer of the OSI reference model **40A** of a first computer **10** and transmitted by the physical layer of the first computer **10** to the physical layer of a first interface device **16**, where the data is packetized according to standard TCP/IP protocols and further encrypted at the network or IP layer **42A**

Further, once data has been packetized and encrypted at the IP layer, Droge discloses that it may be sent out over a packet switching network **22**, such as, the Internet, *where it is retrieved by a second interface device **24** that decrypts the data at the network or IP layer of an OSI reference model **42B** using an IP layer decrypting algorithm that is the reverse of the encrypting*

[2] Droge at ABSTRACT.

*algorithm used by network or IP layer **42A** of the first interface device **16** to encrypt the data.*

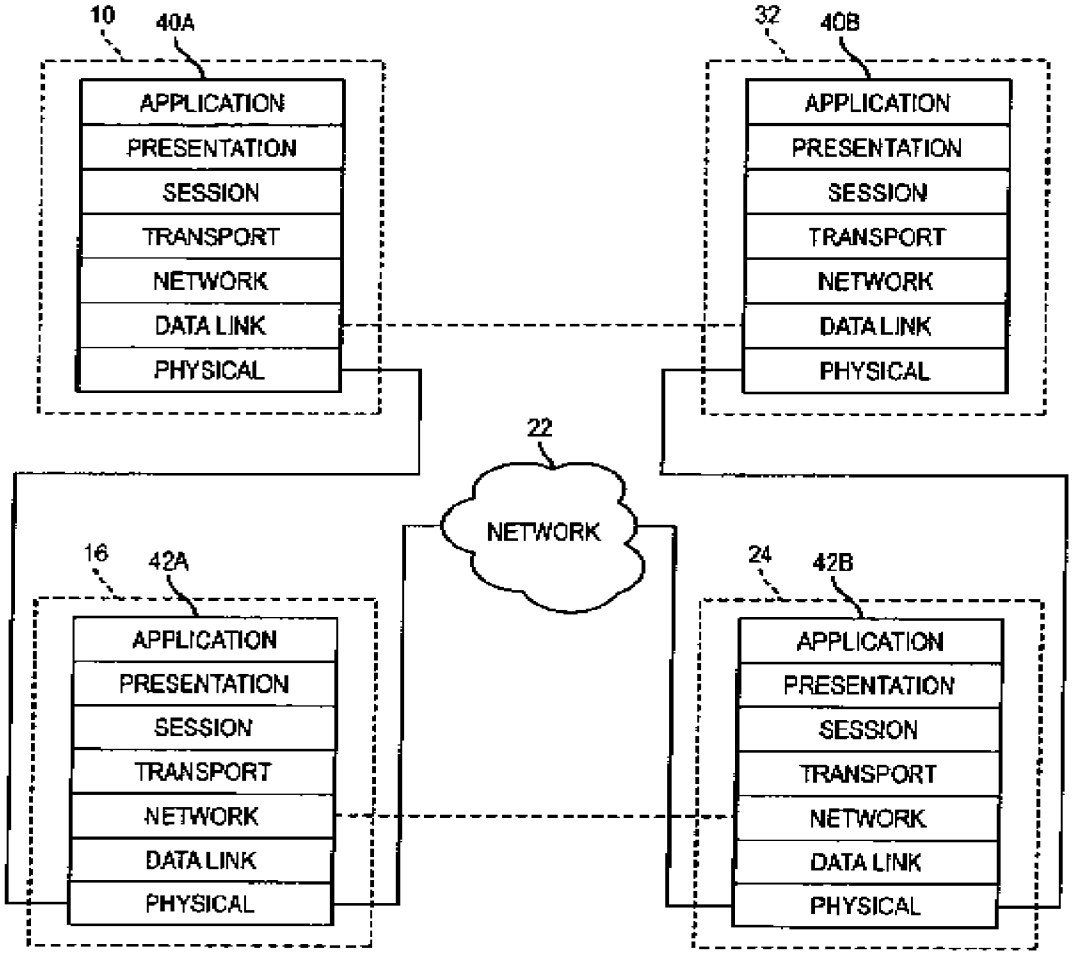


FIG. 3

Furthermore, as shown in **FIG. 3**, Droge discloses the data, which at this stage of transmission is no longer IP layer encrypted but only data link layer encrypted is then reconstructed, or depacketized and then transmitted from the physical layer of the OSI reference model **42B** of the second interface **24** to the physical layer of the OSI reference **40B** of a second computer **32**, where it is decrypted at the data link layer **40B** using a data link layer decrypting algorithm that is the reverse of the encrypting algorithm used by the first computer **10** to encrypt the data. At this stage, the data is no longer encrypted and is available for use by a user.

However, Droge nowhere discloses, as amended claim 1 recites:

> bridge means in a data link layer for allowing data, which has been received with one of the plurality of ports and then on which the encrypting or decrypting process has been performed, to be outputted as it is from another port *without any routing process at a network layer being performed* (emphasis added).

Independent claims 3 and 5 recite similar limitations. That is, as discussed above, **Droge** discloses routing processes at the network layer of the OSI reference model are being performed between the first interface **16** and the second interface **24** of **FIG. 3** above, which are analogous to the claimed apparatus and method. Thus, Droge not only does not disclose the claimed limitations it also teaches away from the claimed invention which recites: "encrypting or decrypting process has been performed, to be outputted as it is from another port without routing processes at a network layer being performed."

In addition, neither Funabe et al. nor Droge disclose, as new claims 9-11 recite: "wherein the bridge means is an IP-Sec bridge and data transmission processes are carried out in layers lower than the network layer."

Further, Droge discloses that encryption at the data link layer **40A** may be effected using *any data link layer encryption mechanism*, including, without limitation, devices implementing data link layer encryption techniques currently available on the market such as the Mykotronx PALLADIUM or KIV-7 or the Cylink LINK ENCRYPTOR (emphasis added).[3] Further, Droge discloses *encryption at the network or IP layer **42A** of first interface **16** may be effected using any IP layer encryption technique*, such as, for example, an Internet Protocol (IP) packet encryption method *such as IPSec* (emphasis added).[4] Moreover, Droge discloses *algorithms that may be used to encrypt data at both the data link and IP layers* include, without limitation, the DATA ENCRYPTION STANDARD (DES), TRIPLE DES, the ADVANCED ENCRYPTION STANDARD (AES), SKIPJACK and BLOWFISH.[5] Thus, it is respectfully submitted that Droge does not disclose "IPSec" as a "data link layer encryption mechanism" or the IP-Sec bridge" as claimed in the present invention. Moreover, Droge does not disclose IP-Sec as "an algorithm that may be used to encrypt data at both the data link and IP layers," as explicitly

[3] *Id.* at column 7, lines 1-5.
[4] *Id.* at column 7, lines 1-5.
[5] *Id.* at column 7, lines 9-14.

disclosed by Droge above but instead suggests IP Sec is a network or "IP layer encryption technique." *That is, Droge* also teaches away from this aspect of the claimed invention.

Thus, Droge cannot overcome all of the deficiencies of Funabe et al. Therefore, it is respectfully submitted that neither Funabe et al. nor Droge, whether taken alone or in combination, disclose, suggest or make obvious the claimed invention and that claims 1, 3 and 5, and claims dependent thereon, patentably distinguish thereover.

Conclusion

In view of the above amendment, applicant believes the pending application is in condition for allowance.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 22-0185, under Order No. 27592-01102-US1 from which the undersigned is authorized to draw.

Dated: January 6, 2009

Respectfully submitted,

Electronic signature: /Myron Keith Wyche/
Myron Keith Wyche
Registration No.: 47,341
CONNOLLY BOVE LODGE & HUTZ LLP
1875 Eye Street, NW
Suite 1100
Washington, DC 20006
(202) 331-7111
(202) 293-6229 (Fax)
Agent for Applicant